Department of Health and Human Services
Office of the Commissioner
Policy and Procedure Statement

Policy # DHHS-06-04

Issue Date: 07/01/04
Revised Date: 11/14/05

I. SUBJECT

Policy Concerning the Use of State Automation Equipment

II. POLICY STATEMENT

The purpose of this statement is to establish policies and procedures to be followed while using any or all of the State automation equipment under the control of the Maine Department of Health and Human Services (DHHS), and is consistent with all state-wide policies related to information technology issued by the State's Chief Information Officer. (www.maine.gov/cio/ispd/index.htm).

III. RATIONALE

This policy statement has been adopted in order to provide guidance and protection to DHHS employees and to safeguard the technological assets of the State entrusted to DHHS employees. DHHS provides its employees access to State automation equipment to accomplish tasks, processing, and communications necessary to effectively achieve DHHS' mission, as directed by law and the administration. **State automation equipment is made available to employees to conduct official DHHS business.** Unofficial and/or unauthorized use of State automation equipment places unanticipated and possibly excessive demands on the State's Information Technology (I.T.) resources and may violate the privacy rights of individuals. Accessing unofficial and/or unauthorized sources unnecessarily exposes the State to the spread of computer viruses, which may be both costly and disruptive to clean from DHHS I.T. and related systems.

IV. PROCEDURE STATEMENT

A. Security of Information

DHHS employees are hereby made aware that cell phones and Internet messages are generally not secure and can be easily intercepted by outside parties. Care shall be exercised to avoid inadvertent disclosure of confidential or personal/protected health information (PHI) over these media. **Employees are advised that there should be no expectation of privacy when using any State automation equipment.** Non-crypted cell phones and unsecured/non-encrypted Internet connections **must not** be used to discuss or disclose any PHI (such as HIV status, substance abuse status/treatment, mental health condition(s), etc.)

B. Health Insurance Portability and Accountability Act (HIPAA), Administrative Simplification and Other Confidentiality Laws.

HIPAA is a federal law that governs the access and distribution of PHI and provides guidance on what measures are needed to safeguard that information. There are many other federal or state laws that make certain information confidential, such as, child and adult protective information, eligibility information regarding federally funded benefit programs, etc. In general it is everyone's responsibility to protect access to PHI and other confidential information and maintain a high level of confidentiality around this information. Only those employees that have a "need to know" basis should be involved with PHI or other confidential information. Employees should be taking reasonable precautions to protect PHI or other confidential information and not to divulge this information to unauthorized third parties or other employees who do not have "need to know" access. Reasonable (non-technological) precautions include, but are not limited too, not discussing PHI or other confidential information in public areas, not discussing this information with non-authorized employees, not discussing this information with family and friends, not leaving computer screens on that are viewing PHI or other confidential information, not having computer monitors set up so that they are easily readable from a door, window, etc., not sending out e-mails or faxes over known unsecured lines, not removing PHI or other confidential information from the premises when not authorized to do so, not using other person's passwords, etc.

C. Public Information

E-mail systems, Internet and Worldwide Web browsers, bulletin board systems, etc., are intended to be used for State business purposes. Voice mail and e-mail messages may have backup copies that cannot be deleted by the operator. A history of accessed web sites is recorded by most browser software. All material created, modified, stored, moved, distributed, transferred, printed, imaged, or otherwise manipulated on State automation equipment is considered to be public property and, as such, is subject to examination by the public, except as noted below. PHI and other information made confidential by statute are not considered public information.

D. Freedom of Access Law

All non-confidential information may be subject to release under a "Freedom of Access Law" request. The State of Maine "Freedom of Access Law" (1 MRSA, § 401-434) clearly provides that any and all materials, files, notes, records, copies, etc., regardless of the media used to store or transmit them (paper, film, microfiche, magnetic media, electronic media, etc.) in public offices or in the possession of public employees while at work which relate in any way to the transaction of public or governmental business are public property. As such, the public has access to those materials.

Although the law places some very narrow restrictions on public access; such as personnel files, employment applications, employee testing and rating criteria, workers' compensation files, certain investigation files, etc. most materials are subject to public viewing.

E. Use of Automation Equipment

1. The use of State automation equipment to create, record, store, transmit, distribute, image, modify, print, download, or display inappropriate or unprofessional materials that demean, denigrate, or harass individuals or groups of individuals, on the basis of race, ethnic heritage, religious beliefs, disability, age, sexual orientation, political beliefs, gender, and/or materials that are sexually explicit or pornographic in nature, whether or not the material was intended to demean, denigrate or harass any employee or group of employees, is prohibited.

2. The State's E-mail is not to be used to forward or otherwise broadcast "chain letters," mass communications that are not work related, or solicitations for causes unrelated to the State's business, no matter how worthy the cause may be perceived. [NOTE: In the Capitol area, Capitol Security must give written permission for solicitations.] The *Maine State Employees Combined Charitable Appeal* is the only solicitation with on-going, or "blanket" approval. Other charitable solicitations may be allowed only on prior written approval of the Commissioner, and Capitol Security where applicable.

3. All e-mail messages sent by an employee will contain the confidentiality notice specified and approved by the Commissioners Office. If an employee sends or receives an E-mail message(s) that contains PHI or other confidential information, the message needs to have a “Confidential PHI Enclosed” or “Confidential Information Enclosed” label placed into the Subject line (for sent messages) or at the top of the actual message (for received messages), in bold letters.

4. E-mail messages and Internet sites accessed are not private but are property of the Department. The Department may print and review e-mail messages and Internet sites accessed by an employee’s system.

5. State automation equipment may not be used to conduct outside business nor may it be used in conjunction with any outside employment activity.

6. Any personal use of State automation equipment must be incidental in nature. Examples of incidental use may include, but are not limited to, brief e-mails, accessing an appropriate subject on the Internet, phone calls of an urgent nature, using computer capabilities for brief correspondence, etc. The personal use of any State-owned telephones made to or from a State-owned cell that results in costs incurred by the State (i.e. long distance personal phone calls or any personal calls made

to or from a State-owned cell phone) must be reimbursed by the employee. Certain telephone calls and expenses are allowable under collective bargaining agreements. The use of State-owned supplies represents a cost to the State and, as such, printing and copying for personal use is restricted to incidental use only.

7. Any personal, incidental use of State automation equipment shall not interfere with the DHHS' business activities, must not involve solicitation in any form, must not be associated with any outside business or employment activity, and must not potentially embarrass or offend the State of Maine, its residents, its taxpayers, or its employees. As is the case in other situations, the time associated with any incidental personal use of State automation equipment must not intrude into an employee's work responsibilities.

8. An employee will not at any time, without a person's permission, use another's identity to send or receive e-mail. An employee will likewise not retrieve messages or files intended for another without the approval of Department management.

9. If an employee uses a personal computer that is not provided by the Department, for State business purposes, the PC must have installed and operating the current version of the State-approved anti-virus product. Any service or support of personal hardware is solely the responsibility of the owner, not the Department. The personal computer **must not** be used to access, download or store PHI or other confidential information.

10. The State's E-mail is not to be used to forward or otherwise broadcast virus warnings or other computer system related announcements. The Office of Technology Management Services is the only unit authorized to disseminate this information to Department Employees. If you feel you have received information that should be broadcast to some or all of the Department employees, contact the Director of the Office of Technology Management Services.

11. Personal software will not be permitted on State automation equipment. However, single user non-networked applications that require no communications, i.e. stand-alone PC applications, may be loaded for evaluation by a qualified, OTMS-approved technician with prior approval from both:

    - The Office of Technology Management Services (OTMS)
    - The appropriate supervisor

    The technician must review the software prior to installation and is responsible for its support during the evaluation. An evaluation period must comply with all licensing requirements and in no case be longer

than ninety (90) days, after which the technician must remove the software. Should the product prove desirable, standard acquisition guidelines and procedures apply.

12. At no time shall any employee, other than a qualified OTMS-approved technician, open, insert, remove or alter any hardware comprising State automation equipment. All configuration changes to State automation hardware or software will be done only by qualified, OTMS-approved technicians.

13. Personal hardware will not be permitted on State automation equipment unless installed by a qualified, OTMS - approved technician with prior approval from both:

    - The Office of Technology Management Services (OTMS)
    - The appropriate supervisor

    Any service or support of personal hardware is solely the responsibility of the owner, not the Department.

14. No streaming video or audio applications including, but not limited to, weather or satellite maps, stock market updates, news headlines, any service that continually updates your PC, TV channels on the Internet, music videos, movie or entertainment broadcasts, radio music or news broadcasts, live interviews or non-critical audio/video seminars are allowed if not directly needed in the performance of assigned duties.

15. No third-party games may be loaded, downloaded or used on any DHHS equipment. Those games which may come as part of standard software, i.e. operating systems, etc., must be removed by qualified technical employees prior to distribution to Department employees.

16. Screensavers may be changed to suit personal taste provided they do not add software or conflict with the Department's mission or other portions of this policy. Use of a screensaver that is licensed or copyrighted is prohibited.

17. Any type of removable storage discs, such as floppy disks, cd's, zip disks etc, that contains PHI or other confidential information are at no time allowed to be removed from the premises, unless the employee has written authorization from their supervisor to do so, is authorized to do so as part of his or her job function, or is transporting the data to another site that has authorization to view/use the PHI or other confidential information. Removable storage media used to transport confidential information will be protected from inadvertent disclosure in case of loss or theft by password protection or encryption.

18. At no time will an employee make duplicate copies of PHI or other confidential information, unless the employee has written authorization from his or her supervisor to do so, is authorized to do so as part of his or her job function, or back-up copies are being made as part of a Disaster Recovery Plan or Emergency Mode Operation Plan.

F. Guidelines And Procedures

1. In the event that an employee is sent, delivered or inadvertently accesses inappropriate or prohibited material, or the material contains PHI or other confidential information that the employee does not have need to know access to, or authority to receive, the employee is required to immediately secure the material from view and notify their supervisor. If an employee inadvertently accesses inappropriate or prohibited materials, or the material contains PHI or other confidential information that the employee does not have need to know access to or authority to receive, his or her supervisor or management must be advised of the circumstances surrounding the inadvertent access and must file an Incident Report with their supervisor within 48 hours. This will ensure that the employee is held harmless for inadvertently accessing the inappropriate or prohibited materials. In addition, any departmental employee having knowledge of any potential unauthorized disclosure must promptly report the incident of disclosure to the appropriate departmental official with HIPPA privacy responsibilities.

2. If supervisory or management employees become aware that inappropriate or prohibited materials are being accessed, downloaded, or otherwise transmitted to or by an employee in his or her organization, he or she must act immediately to stop such activity. Supervisors and managers should contact the Human Resources Director, DHHS, for guidance and consultation.

3. Each DHHS employee is expected to comply with this policy. Violation of this policy may lead to progressive discipline, up to and including dismissal consistent with applicable collective bargaining agreement and/or Civil Service Rules.

4. DHHS employees and the Department of Administrative & Financial Services, Bureau of Information Services may monitor voice, e-mail, and Internet traffic to improve service levels, enforce this policy, and prevent unauthorized access to State systems. The Department will review and document the risk and vulnerability of PHI that is sent electronically and will implement whatever safeguards are necessary in order to prevent the unauthorized use or disclosure of such PHI.

5. These rules may be amended as necessary by State policies and procedures or by updated DHHS policies.

6. Employees needing further clarification regarding the technical aspects of this policy may contact the Director of Technology Management Services, DHHS (287-3864). For questions regarding the policy and its implementation, employees may contact the Director of Human Resources, DHHS (287-2567).

V. DEFINITIONS

Protected Health Information (PHI): Individually identifiable health information: Any identifiable health information included in the HIPPA Privacy Rule definition at C.F.R.§164.501 and also including any protected health information which is either transmitted by electronic media, maintained in any medium described in the definition of electronic media in the HIPPA Electronic Data Interchange Rule, 45 C.F.R.§162.103, or transmitted or maintained in any other form or medium.

Health information: Any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

State Automation Equipment: State automation and related communications equipment may include, but are not limited to: Computer workstations, computer terminals, laptop, notebook and hand-held computers, voice mail, computer networks, printers, copiers, telephones, fax machines, modems, fax modems, wireless modems, e-mail, local and wide area networks, Internet, and Intranet.

Public Records: Public records include all e-mail messages and attachments, information obtained from the Internet, and all other electronic transmittals which have been created, received, or stored on State of Maine automation equipment including all such public records as defined by (1 MRSA §402(3).

Public Disclosure: All public records are subject to administrative review, inspection by the public, and discovery requests as part of legal proceedings in accordance with (1 MRSA §402). Incidental personal use records may be subject to disclosure if stored on Department IT equipment.

Incidental Use: The use of State automation equipment for personal use must be infrequent and using only small amounts of an employee's personal time either inside or outside the regular work day. Occasional use during an employee's break would be considered incidental. Any use that interferes with or slows the completion of the Department's business would not be considered incidental. Only occasional and brief use is considered incidental. Any incidental use must be consistent with Section IV, E.

VI. DISTRIBUTION

Current employees shall, following the appropriate posting, receive a copy of this policy.

New employees shall receive a copy of this policy upon hire.

Each employee shall sign a statement, confirming that his/her copy of this policy has been received and read. (Refer to Attachment.)

Said statement (Attachment) shall be filed in employee's personnel folder.

VII. ATTACHMENTS

Employee Use of State Automation Equipment Acknowledgement Form

11/14/05
Date of Revision

John R. Nicholas
Commissioner

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Employee Use of State Automation Equipment Acknowledgment

I acknowledge that I received, read and understand a copy of the Department of Health and Human Services Policy "USE OF STATE AUTOMATION EQUIPMENT" dated November 14, 2005.

Employee's name (please print): _____

Signature: _____Date: _____

Office/Division_____